IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
MIDLAND/ODESSA DIVISION

Secure Matrix LLC, Plaintiff, v. **Santikos Real Estate Services, LLC,** Defendant.	Case No. 7:25-cv-00120-DC- DTG Patent Case Jury Trial Demanded

PLAINTIFF'S RESPONSE IN OPPOSITION TO
DEFENDANT SANTIKOS REAL ESTATE SERVICES, LLC'S
RULE 12(b)(6) MOTION TO DISMISS FOR FAILURE TO STATE A CLAIM

Plaintiff Secure Matrix, LLC ("Secure Matrix" or "Plaintiff") submits this brief in opposition to the Defendant Santikos Real Estate Services, LLC ("Santikos" or "Defendant") Rule 12(b)(6) Motion to Dismiss (the "Motion") filed on May 5, 2025 (Dkt. No. 15). For the reasons set forth below, the Motion should be denied.

I. INTRODUCTION

Defendant's Motion attempts to characterize the '116 Patent as claiming nothing more than the abstract idea of "authentication," but this oversimplification ignores the specific technical implementation that addresses concrete technological deficiencies in prior authentication systems. As argued herein and alleged in Plaintiff's First Amended Complaint ("FAC"), Claim 1 of the '116 Patent represents an advancement in computer security technology that improves both security and efficiency through its innovative combination of time-limited reusable identifiers with user verification information. Unlike the authentication technologies found ineligible in cases cited by Defendant, the '116 Patent claims a specific technique that departs from earlier approaches to solve particular technical problems of the prior art—exactly the kind of technological improvement that the Federal Circuit found patent-eligible. The '116

Patent time-sensitive approach using reusable identifiers provides concrete benefits, including prevention of replay attacks, universal updating across platforms, and reduced system resource expenditure for credential management. These are not abstract benefits, but specific improvements to authentication technology and to computer functionality itself.

As argued herein, Defendant's Motion is premature in that it raises factual disputes with Plaintiff's FAC regarding whether the claimed technology was conventional, and lacks merit given the clear eligibility of the '116 Patent.

Accordingly, Defendant's Motion should be denied. In the alternative, Plaintiff would ask for leave to amend.

II. TECHNICAL BACKGROUND OF THE '116 PATENT

Prior to the invention of the '116 Patent, conventional systems and methods for authenticating users seeking to conduct interactions with secured capabilities were ineffective and vulnerable to security breaches. Dkt. No. 14 at ¶ 10. These conventional systems typically relied on simple username and password mechanisms that could be easily compromised through various attacks, rendering security protection inadequate once breached. *Id.*

The conventional authentication solutions of the prior art had several technological deficiencies. For example, conventional solutions were dependent on users remembering "a multitude of passwords" with "different password requirements" for multiple websites, which frequently resulted in significant costs spent on "customer support services for lost and forgotten passwords." Dkt. No. 14 at ¶ 11 (quoting '116 Patent, 32:63-33:2).

Prior art authentication methods also depended on static, single-factor authentication mechanisms that were readily susceptible to compromise. This technical approach was fundamentally flawed because once a password was obtained by an unauthorized user, the protection was entirely lost, and the user would need to "notify [each] other website" individually when security was compromised. Dkt. No. 14 at ¶ 12 (quoting '116 Patent, 33:6-9).

The '116 Patent addressed these technological deficiencies by providing computer systems and methods for "authenticating a user seeking to conduct at least one interaction with a secured capability." Dkt. No. 14 at ¶ 13 (quoting '116 Patent, 1:29-31). The invention recognized that authentication could be improved through a multi-factor approach utilizing "reusable identifiers" in combination with "user verification information" that is derived from user-specific or device-specific data. '116 Patent, Claim 1.

To address the technological deficiencies of conventional systems and methods, and to provide enhanced security, the '116 Patent claims unconventional and inventive systems and methods implementing a reusable identifier authentication system that provides multiple layers of security protection. Dkt. No. 14 at ¶ 14. The claimed invention provides an approach that maintains protection by utilizing a "reusable identifier corresponding to the secured capability" that is assigned for use "for a finite period of time," and combining this with "user verification information" that can include both user-specific and device-specific information. '116 Patent, Claim 1. *Id*.

The systems and methods claimed in the '116 Patent represent an architectural advancement in computer security technology by providing a protection mechanism that maintains security integrity through a unique combination of reusable identifiers and user verification information. Thus, the claimed invention implements an approach to authentication that was not previously available in conventional systems. Dkt. No. 14 at ¶ 15 (citing '116 Patent, 32:56-60 ("By using reusable identifiers that do not include user specific or transaction specific information, certain embodiments described herein can advantageously provide a universal login or universal payment application that can work on every website and can provide an exceptional user experience.")).

Rather than simply computerizing pre-existing processes, the '116 Patent claims specific implementations not previously available in the prior art, wherein authentication is enhanced through an inventive and unconventional multi-factor approach that improves security while

simultaneously enhancing user experience. Dkt. No. 14 at ¶ 16. As the '116 Patent explains, the invention provides "a level of safety over a million times greater than systems that utilize just a login and password." *Id.* (quoting '116 Patent, 33:3-4).

The authentication systems and methods claimed in the '116 Patent improved computer functionality by integrating a reusable identifier with user verification information to create a more robust and efficient authentication framework that prior art solutions could not provide. Dkt. No. 14 at ¶ 17. This unconventional and inventive approach permits secure authentication across multiple platforms while eliminating the need for users to remember multiple passwords or for companies to maintain expensive customer support services for lost credentials. *Id.* (quoting '116 Patent, 32:56-33:4).

As the '116 Patent explains, the invention provides significant advantages, as "all the supporting websites will immediately work with the new PIN when a user changes the PIN on his smartphone, and the user does not need to notify any other website, as would be needed for systems that utilize passwords." Dkt. No. 14 at ¶ 18 (quoting '116 Patent, 33:6-9). This capability means that the authentication system can be updated universally and efficiently without requiring changes to multiple websites or systems, even during execution. *Id.*

The inventive concepts of the '116 Patent provided a superior a technical solution to the technical problem of authentication, sparing computer system resources from being expended on password recovery and maintenance, reducing the risk of compromised accounts, and creating a uniform authentication system that works across multiple platforms. Dkt. No. 14 at ¶ 19.

A further key focus of the claimed advance is the assignment of the reusable identifier "for a finite period of time," the correlation of signals received within this time window, and the evaluation of authorization based on this time-sensitive approach. Dkt. No. 14 at ¶ 20. The '116 Patent's time-limited reusable identifier represents a concrete improvement over conventional authentication systems. As explained in the specification, when using the processor to evaluate authorization, the system can determine "a first time of receipt of the first signal and a second

time of receipt of the second signal, and can compare the time differential between the first time and the second time." *Id*. (quoting '116 Patent, 13:29-33). For example, specification further explains that "if the time differential is less than or equal to the finite and predetermined period of time for the reusable identifier... the validation server 60 can evaluate that the user 10 is authorized," while "if the time differential is greater than the finite and predetermined period of time... the validation server 60 can evaluate that the user 10 is not authorized." *Id*. This time-sensitive approach provided a superior technological solution as compared to conventional systems and methods in that it prevented replay attacks where an intercepted identifier might be used at a later time by an unauthorized party. *Id.*

Moreover, the implementation of a time-limited reusable identifier provides a specific technological improvement over conventional systems by both enhancing security and maintaining user convenience. Dkt. No. 14 at ¶ 21. The specification explains how the reusable identifiers can be "only valid for a finite and predetermined period of time (e.g., one or more minutes, one or more hours, one or more days) but can be used in multiple such periods of time." *Id.* (quoting '116 Patent, 9:42-46). This approach allows the system to implement a "round robin" usage of identifiers where "after the period of time has elapsed, the verification server 60 deletes the record corresponding to the reusable identifier 214 so it can be reused again" without "performing any timestamp comparison." *Id*. (quoting '116 Patent, 13:43-45). This specific technical implementation represents a concrete improvement that increases computer and network security by preventing unauthorized access through expired credentials, while simultaneously reducing system complexity and computer resource usage by enabling reuse of identifiers in a controlled, secure manner.

These inventive concepts are captured in the limitations of Claim 1 reciting steps of "using the computer system to receive a first signal from the computer providing the secured capability, the first signal comprising a reusable identifier corresponding to the secured capability, the reusable identifier assigned for use by the secured capability for a finite period of

time," "using the computer system to receive a second signal from an electronic device being used by the user, the second signal comprising a copy of the reusable identifier and user verification information," and "using a processor to evaluate, based at least on the first signal and the second signal, whether the user is authorized to conduct the at least one interaction with the secured capability." These steps require the inventive and unconventional secure authentication protocol utilizing reusable identifiers and user verification information to significantly enhance computer security. Dkt. No. 14 at ¶ 22.

None of the methods or systems of the '116 Patent were previously performed by human beings, or capable of being performed in the human mind, as they necessarily involve complex computer systems communicating through network protocols to implement a multi-factor authentication system using reusable identifiers and user verification information within specific time periods. Dkt. No. 14 at ¶ 23.

III. ARGUMENT

A. Defendant's Section 101 Arguments Are Premature and Raise Disputed Issues of Fact That Preclude Resolution of Section 101 Issues at the Pleading Stage

The analysis of patent-eligibility under 35 U.S.C. § 101 involves "question[s] of fact," such as "whether a claim element or combination of elements is well-understood, routine and conventional to a skilled artisan in the relevant field." *Berkheimer v. HP Inc*., 881 F.3d 1360, 1368 (Fed. Cir. 2018). Thus, "plausible and specific factual allegations that aspects of the claims are inventive are sufficient" to "defeat[] a motion to dismiss." *Cellspin Soft, Inc. v. Fitbit, Inc*., 927 F.3d 1306, 1317 (Fed. Cir. 2019) (stating that "factual disputes about whether an aspect of the claims is inventive may preclude dismissal at the pleadings stage under § 101," and noting that "[w]e have no basis, at the pleadings stage, to say that these claimed techniques, among others, were well-known or conventional as a matter of law"); *see also Aatrix Software, Inc. v. Green Shades Software, Inc*., 882 F.3d 1121, 1126–27 (Fed. Cir. 2018) (finding factual allegations of patentee's complaint were sufficient to survive a motion to dismiss and stating that

"patentees who adequately allege its claims contain inventive concepts survive a § 101 eligibility analysis under Rule 12(b)(6)"). Therefore, where a disputed issue of fact relevant to the analysis of patent-eligibility under Section 101 exists, eligibility may not be resolved at the pleading stage.

Many courts have found that "the issue" of eligibility under Section 101 "is inherently ill suited to adjudication at the pleading stage, particularly when the dispute turns on whether the claims are impermissibly abstract," as here. *Ubiquitous Connectivity, LP v. Cent. Sec. Grp. - Nationwide, Inc*., No. 18-CV-368-JED-CDL, 2021 WL 1970664, at *3–4 (N.D. Okla. May 17, 2021). "'Determining patent eligibility requires a full understanding of the basic character of the claimed subject matter'…but the two tools mostly likely to aid the court in developing such an understanding—claim construction and the presentation of expert testimony—will not ordinarily have occurred at the dismissal stage." *Id.* (quoting *MyMail, Ltd. v. ooVoo, LLC*, 934 F.3d 1373, 1379 (Fed. Cir. 2019)). Further, the "*Alice* test is notoriously difficult to apply, even in the best of circumstances. In a recent survey of judges who frequently handle patent cases, respondents rated eligibility under § 101 to be the most difficult issue of patent validity and the area of patent law with the least doctrinal clarity." *Id*. (citing Matthew G. Sipe, *Patent Law 101: The View From the Bench*, 88 Geo. Wash. L. Rev. Arguendo 21, 29 (2020)). "When this task is undertaken at the pleading stage, where a court cannot benefit from the claim construction process and a developed factual record, accuracy will be the exception rather than the rule." *Id*.

Indeed, as this Court itself has warned, "[r]esolving validity issues at the Rule 12 stage can also tempt courts, sometimes improperly, to conclude that certain concepts are conventional or routine by way of judicial notice." *Intellectual Ventures II LLC v. FedEx Corp.*, 2017 WL 6002762, at *2 n. 1 (E.D. Tex. 2017) (Gilstrap. J.).

For these reasons, many courts have found "it is wiser and more efficient to wait to determine a patent's § 101 eligibility until after fact discovery has opened" and "after issuing its claim construction order." *Slyce Acquisition Inc. v. Syte - Visual Conception Ltd.*, No. W-19-CV-

257, 2020 WL 278481, *3–7 (W.D. Tex. Jan. 10, 2020) (noting, *inter alia*, that "a Rule 12(b) motion to dismiss is a procedurally awkward place for a court resolve a patent's § 101 eligibility"); *see also e-Numerate Sols., Inc. v. United States,* 149 Fed. Cl. 563, 577–79 (2020) (accord).

As argued further herein, Defendant's Motion is premature in that it raises factual issues that would benefit from a more developed record, and should be denied on that basis alone. In particular, Defendant raises a factual dispute regarding whether methods implementing a reusable identifier authentication system that provides multiple layers of security protection and utilizes a time-sensitive approach, especially one using a reusable identifier for a "finite period of time," were somehow "well-understood, routine and conventional" at the time of invention.

B. The '116 Patent is Directed to Patent-Eligible Subject Matter

Defendant presents a significant oversimplification of the '116 Patent's claims, arguing that they are directed to the abstract idea of "authentication." Dkt. No. 15 at 9. However, this characterization fails to account for the specific requirements of the claims and improperly frames the analysis. Because "all inventions ... embody, use, reflect, rest upon, or apply laws of nature, natural phenomena, or abstract ideas," *Mayo Collaborative Servs. v. Prometheus Labs.*, 566 U.S. 66, 71 (2012), "courts 'must be careful to avoid oversimplifying the claims' by looking at them generally and failing to account for the specific requirements of the claims[,]" *McRO Inc. v. Bandai Namco Games Am. Inc.*, 837 F.3d 1299, 1313 (Fed. Cir. 2016); *see also Enfish, LLC v. Microsoft Corp*., 822 F.3d 1327, 1337 (Fed. Cir. 2016) ("[D]escribing the claims at [too] high [a] level of abstraction and untethered from the language of the claims all but ensures that the exceptions to § 101 swallow the rule.").

The claims of the '116 Patent are not, as Defendant suggests, directed merely to the abstract idea of "authentication." Rather, they are directed to a specific implementation of an authentication system that provides multiple layers of security protection in an inventive and unconventional way. As alleged in the FAC, the '116 Patent "addressed the technological

deficiencies [of conventional systems] by providing computer systems and methods for 'authenticating a user seeking to conduct at least one interaction with a secured capability.'" Dkt. No. 14 at ¶ 13. The systems and methods claimed in the '116 Patent "represent an architectural advancement in computer security technology by providing a protection mechanism that maintains security integrity through a unique combination of reusable identifiers and user verification information." *Id.* at ¶ 15.

Unlike the authentication technologies found ineligible in cases cited by Defendant, the '116 Patent claims a specific technique for solving a specific computer problem. As alleged, the invention "improved computer functionality by integrating a reusable identifier with user verification information to create a more robust and efficient authentication framework that prior art solutions could not provide. This unconventional and inventive approach permits secure authentication across multiple platforms while eliminating the need for users to remember multiple passwords or for companies to maintain expensive customer support services for lost credentials." Dkt. No. 14 at ¶ 17.

The present case is analogous to *Ancora Technologies, Inc. v. HTC America, Inc.*, 908 F.3d 1343 (Fed. Cir. 2018), where the Federal Circuit held claims directed to improving computer security to be patent-eligible. In *Ancora*, the court emphasized that the claims were "directed to improving a basic function of a computer data-distribution network, namely, network security" through "a specific technique that departs from earlier approaches to solve a specific computer problem." *Id*. at 1348. Similarly, as alleged in the FAC, the inventive concepts of the '116 Patent provide "a superior technical solution to the technical problem of authentication, sparing computer system resources from being expended on password recovery and maintenance, reducing the risk of compromised accounts, and creating a uniform authentication system that works across multiple platforms." Dkt. No. 14 at ¶ 19.

A key focus of the claimed advance is "the assignment of the reusable identifier 'for a finite period of time,'" the correlation of signals received within this time window, and the

evaluation of authorization based on this time-sensitive approach, captured in the "finite period of time" limitation of Claim 1. Dkt. No. 14 at ¶ 20. The time-limited reusable identifier "represents a concrete improvement over conventional authentication systems" by preventing replay attacks where an intercepted identifier might be used at a later time by an unauthorized party.

Unlike the patents in *Universal Secure Registry LLC v. Apple, Inc.*, 10 F.4th 1342 (Fed. Cir. 2021), the '116 Patent, as alleged, provides sufficient specificity to constitute an improvement to computer functionality itself. As explained in the Amended Complaint, the implementation of a time-limited reusable identifier "provides a specific technological improvement over conventional systems by both enhancing security and maintaining user convenience." Dkt. No. 14 at ¶ 21. The court in *Universal Secure Registry* cautioned that "patent eligibility often turns on whether the claims provide sufficient specificity to constitute an improvement to computer functionality itself." 10 F.4th at 1346. Here, the '116 Patent claims "specific implementations not previously available in the prior art, wherein authentication is enhanced through an inventive and unconventional multi-factor approach that improves security while simultaneously enhancing user experience." Dkt. No. 14 at ¶ 16.

The claims at issue are also distinguishable from those found ineligible in *Riggs Tech. Holdings, LLC v. Cengage Learning, Inc.*, No. 2022-1468, 2023 WL 193162, at *1 (Fed. Cir. Jan. 17, 2023), *Repifi Vendor Logistics, Inc. v. IntelliCentrics, Inc.*, No. 2021-1906, 2022 WL794981, at *2 (Fed. Cir. 2022), *Elec. Commc'n Techs., LLC v. ShoppersChoice.com, LLC,* 958 F.3d 1178, 1181 (Fed. Cir. 2020), and *Dropbox, Inc. v. Synchronoss Techs., Inc.*, 815 Fed. App'x 529, 531 (Fed. Cir. 2020). Unlike those cases, which involved routine authentication methods, the '116 Patent addresses specific technological deficiencies in prior authentication systems. As alleged, conventional systems "typically relied on simple username and password mechanisms that could be easily compromised through various attacks, rendering security protection inadequate once breached." Dkt. No. 14 at ¶ 16. These systems were problematic

because users had to remember "a multitude of passwords" with "different password requirements" for multiple websites, which frequently resulted in significant costs spent on "customer support services for lost and forgotten passwords." *Id.* at ¶ 11.

Moreover, as alleged, the '116 Patent provides significant technological advantages, including the fact that "all the supporting websites will immediately work with the new PIN when a user changes the PIN on his smartphone, and the user does not need to notify any other website, as would be needed for systems that utilize passwords." Dkt. No. 14 at ¶ 18. This capability means that the authentication system can be updated universally and efficiently without requiring changes to multiple websites or systems, even during execution.

Defendant further argues that Claim 1 somehow does not provide sufficient detail as to "how" the claimed method is carried out. Dkt. No. 15 at 12. But the *IBM* court, in considering the "question of how much 'how' must exist in a patent's claim, in order to elevate the claim from the realm of abstraction to that of patent eligibility," held that "claim 1 clearly discloses, at minimum, one level of 'how,' in reciting a specific solution to the patent's identified problem." *Int'l Bus. Machines Corp. v. The Priceline Grp. Inc*., No. CV 15-137-LPS-CJB, 2016 WL 626495, at *12-13 (D. Del. Feb. 16, 2016). Claim 1 of the '116 Patent provides more than sufficient detail about "how" the authentication method is implemented. For example, Claim 1 specifies "using the computer system to receive a first signal from the computer providing the secured capability, the first signal comprising a reusable identifier corresponding to the secured capability, the reusable identifier assigned for use by the secured capability for a finite period of time." This limitation clearly explains how the system obtains the first piece of authentication information—through a signal containing a specifically defined reusable identifier that has a finite validity period, which is one of the claim's inventive concepts. *See* Dkt. No. 14 at ¶ 20 (explaining the superiority of the claim method's time-sensitive approach over conventional prior art methods). The claim further details "using the computer system to receive a second signal from an electronic device being used by the user, the second signal comprising a copy of

the reusable identifier and user verification information." This limitation articulates exactly how the system obtains the second piece of authentication information—through a separate signal from a different device that contains both the reusable identifier and additional user verification information. There is simply no basis for Defendant's assertion that Claim 1 is somehow entirely "functional" or "result-based."

In sum, the '116 Patent is directed to patent-eligible subject matter because it claims a specific implementation of an authentication technique that solves specific technical problems in the field. By oversimplifying and thus misidentifying the basic character of the '116 Patent's claims, Defendant has failed to meet its burden of demonstrating that the claims are directed to an abstract idea.

C. The '116 Patent Claims Patent-Eligible Inventive Concepts

Even if the Court were to find that the claims of the '116 Patent are directed to an abstract idea, the claims nonetheless contain inventive concepts that transform the nature of the claims into patent-eligible applications under *Alice* step two.

Defendant's argument that Claim 1 lacks an inventive concept because it uses "generic hardware and software" is unavailing. Dkt. No. 15 at 14. The Federal Circuit in *BASCOM Global Internet Servs. v. AT&T Mobility LLC*, 827 F.3d 1341, 1350 (Fed. Cir. 2016) has explicitly recognized that "an inventive concept can be found in the non-conventional and non-generic arrangement of known, conventional pieces." As alleged in the FAC, the systems and methods claimed in the '116 Patent represent an "architectural advancement in computer security technology by providing a protection mechanism that maintains security integrity through a unique combination of reusable identifiers and user verification information." Dkt. No. 14 at ¶ 15. The Federal Circuit has found that an unconventional "architecture" has provided an inventive concept. For example, in *Amdocs*, the Federal Circuit found an inventive concept in a "distributed architecture" that solved a "particular technological problem," i.e., "reduced data flows and the possibility of smaller databases." *Amdocs (Israel) Ltd. v. Openet Telecom, Inc.*,

841 F.3d 1288, 1301-1302 (Fed. Cir. 2016). Similarly here, '116 Patent's "unique combination of reusable identifiers and user verification information" shifted the architecture of conventional systems and methods which "depended on static, single-factor authentication mechanisms that were readily susceptible to compromise." Dkt. No. 14 at ¶ 12.

Unlike the abstract authentication methods rejected in previous cases, the '116 Patent claims provide an approach to authentication that was not previously available in conventional systems and which "provided a superior a technical solution to the technical problem of authentication, sparing computer system resources from being expended on password recovery and maintenance, reducing the risk of compromised accounts, and creating a uniform authentication system that works across multiple platforms." Dkt. No. 14 at ¶ 19. "This specific technical implementation represents a concrete improvement that increases computer and network security by preventing unauthorized access through expired credentials, while simultaneously reducing system complexity and computer resource usage by enabling reuse of identifiers in a controlled, secure manner." *Id*. at ¶ 21. "The '116 Patent's time-limited reusable identifier represents a concrete improvement over conventional authentication systems." *Id*. at ¶ 20. "This time-sensitive approach provided a superior technological solution as compared to conventional systems and methods in that it prevented replay attacks where an intercepted identifier might be used at a later time by an unauthorized party." *Id.* These alleged improvements to computer functionality are precisely the kind of inventive concepts that the Federal Circuit has found to satisfy the second step of the *Alice* analysis.

These inventive concepts are captured in the limitations of Claim 1 reciting steps of "using the computer system to receive a first signal from the computer providing the secured capability, the first signal comprising a reusable identifier corresponding to the secured capability, the reusable identifier assigned for use by the secured capability for a finite period of time," "using the computer system to receive a second signal from an electronic device being used by the user, the second signal comprising a copy of the reusable identifier and user

verification information," and "using a processor to evaluate, based at least on the first signal and the second signal, whether the user is authorized to conduct the at least one interaction with the secured capability." These steps require the inventive and unconventional secure authentication protocol utilizing reusable identifiers and user verification information to significantly enhance computer security—particularly, according to the time-sensitive approach of the claimed method, captured in the "finite period of time" limitation of Claim 1.

Defendant confuses the inquiry regarding what is "conventional," which is a separate question from whether technology is merely "known." In *Berkheimer v. HP Inc.*, 881 F.3d 1360, 1369 (Fed. Cir. 2018), the Federal Circuit explained that "whether a particular technology is well-understood, routine, and conventional goes beyond what was simply known in the prior art. The mere fact that something is disclosed in a piece of prior art, for example, does not mean it was well-understood, routine, and conventional."

In any event, Defendant has no basis for asserting that the claimed method was conventional, let alone that it was known, or for contravening the allegations of Plaintiff's FAC. Defendant has "no basis, at the pleadings stage, to say that these claimed techniques, among others, were well-known or conventional as a matter of law," especially when the '116 Patent and Plaintiff's FAC state that they were not. *Cellspin Soft, Inc. v. Fitbit, Inc.*, 927 F.3d 1306, 1318 (Fed. Cir. 2019). Such a determination would involve disputed issues of fact that are inappropriate for resolution at the motion to dismiss stage. The Court should decline Defendant's invitation to "[r]esolv[e] validity issues at the Rule 12 stage," which "can also tempt courts, sometimes improperly, to conclude that certain concepts are conventional or routine by way of judicial notice." *Intellectual Ventures II LLC v. FedEx Corp.*, 2017 WL 6002762, at *2 n. 1 (E.D. Tex. 2017) (Gilstrap, J.).

Accordingly, Defendant's Section 101 arguments are premature in that they hinge on disputed issues of fact. For example, Defendant raises a factual dispute regarding whether methods implementing a reusable identifier authentication system that provides multiple layers

of security protection and utilizes a time-sensitive approach, especially one using a reusable identifier for a "finite period of time," were somehow "well-understood, routine and conventional" at the time of invention, contrary to the allegations of Plaintiff's FAC. In any event, Defendant's arguments wholly without merit and should be rejected.

D. In the Alternative, Leave to Amend Should Be Granted.

To the extent the Court is inclined to grant Defendant's Motion in any respect, the Court should permit leave to amend to allow Secure Matrix to add additional allegations supporting the '116 Patent's eligibility under Section 101. *See Mad Dogg Athletics, Inc. v. Peloton Interactive, Inc*., No. 2:20-CV-00382-JRG, 2021 WL 4206175, at *7 (E.D. Tex. Sept. 15, 2021) ("The Court should freely grant leave to amend, and the district court must have a "substantial reason" to deny a request to amend a pleading.") (citing Fed. R. Civ. P. 15(a)); *Aatrix*, 882 F.3d at 1126; *Lyn-Lea Travel Corp. v. American Airlines, Inc.*, 283 F.3d 282, 286 (5th Cir. 2002)); *Diatek Licensing LLC v. AccuWeather, Inc*., No. 21 CIV. 11144 (JPC), 2023 WL 2632178, at *12 (S.D.N.Y. Mar. 24, 2023) ("the Court will grant Plaintiff leave to file a Second Amended Complaint, in the event that Plaintiff believes it can plead facts that would make plausible the inference that the activities recited in at least one of the Asserted Claims were not well-understood, routine, or conventional… while Plaintiff has already amended the Complaint once, that amendment occurred before the Court's discussion, in this Opinion and Order, of the sort of allegations that would be required for Plaintiff to defeat a motion to dismiss").

Allowing Secure Matrix to amend in order to add additional allegations would not be futile. For example, as to eligibility, as they would support Secure Matrix's position that, at Step Two of the Section 101 analysis, the claimed method uses an inventive and unconventional methods implementing a reusable identifier authentication system that provides multiple layers of security protection and utilizes a time-sensitive approach, in contrast to the prior art which was dependent on "static" mechanisms that were susceptible to compromise. Given that these are issues of fact relating to the Section 101 analysis, and in light of this Court's own warning

against "improperly" "conclud[ing] that certain concepts are conventional or routine by way of judicial notice," it would be appropriate to grant Secure Matrix leave to amend to add allegations regarding the unconventionality of Claim 1 and the inventive concepts captured therein. *Intellectual Ventures II LLC*, 2017 WL 6002762, at *2 n. 1 (E.D. Tex. 2017) (Gilstrap, J.); *Berkheimer*, 881 F.3d at 1368; *Cellspin Soft, Inc.*, 927 F.3d at 1317; *Aatrix*, 882 F.3d at 1126. Moreover, leave to amend is appropriate given that Secure Matrix has not had the benefit of any discussion from the Court regarding allegations relating to eligibility of the '116 Patent. *See Diatek Licensing LLC v. AccuWeather, Inc.*, 2023 WL 2632178, at *12.

IV. CONCLUSION

Accordingly, Defendant's Motion should be DENIED. In the alternative, Secure Matrix would ask that the Court grant leave to amend.

Dated: May 27, 2025

Respectfully submitted,

/s/ Isaac Rabicoff
Isaac Rabicoff
Rabicoff Law LLC
4311 N Ravenswood Ave Suite 315
Chicago, IL 60613
7736694590
isaac@rabilaw.com

Counsel for Plaintiff
Secure Matrix, LLC

CERTIFICATE OF SERVICE

I hereby certify that I caused the foregoing document to be electronically filed with the Clerk of the Court using the CM/ECF system for the Western District of Texas and that ECF system will send a Notice of Electronic Filing to the CM/ECF participants in this case on the 27th day of May, 2025.

/s/ Isaac Rabicoff
Isaac Rabicoff
Rabicoff Law LLC
www.RabiLaw.com
4311 N Ravenswood Ave Suite 315
Chicago, IL 60613
773.669.4590
isaac@rabilaw.com

Counsel for Plaintiff
Secure Matrix, LLC